

Simulated Phishing Attack Using Zphisher in a Controlled Lab

Author: Onaopemipo Olugbemiro

Date: July 2025

Tools used: Kali Linux, Zipisher

Environment: Virtual Box

Objective

The purpose of this lab exercise was to simulate a phishing attack in a controlled and ethical environment using Zphisher, with the aim of understanding the techniques attackers use in social engineering to trick users into revealing sensitive information.

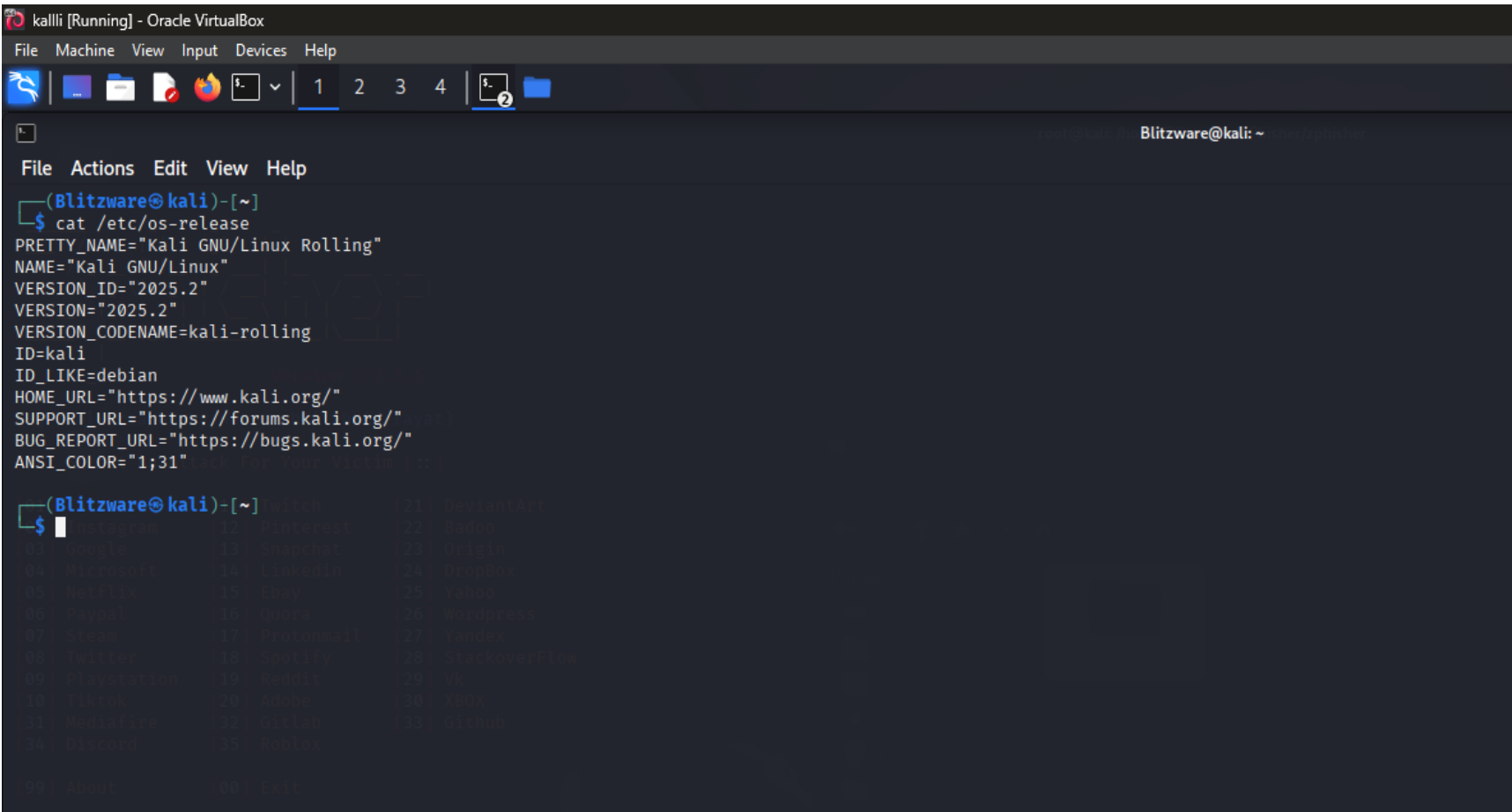
This hands-on simulation helped in exploring the workflow of phishing attacks, learning how phishing pages are hosted, and observing how unsuspecting users could fall for such traps.

Lab Setup

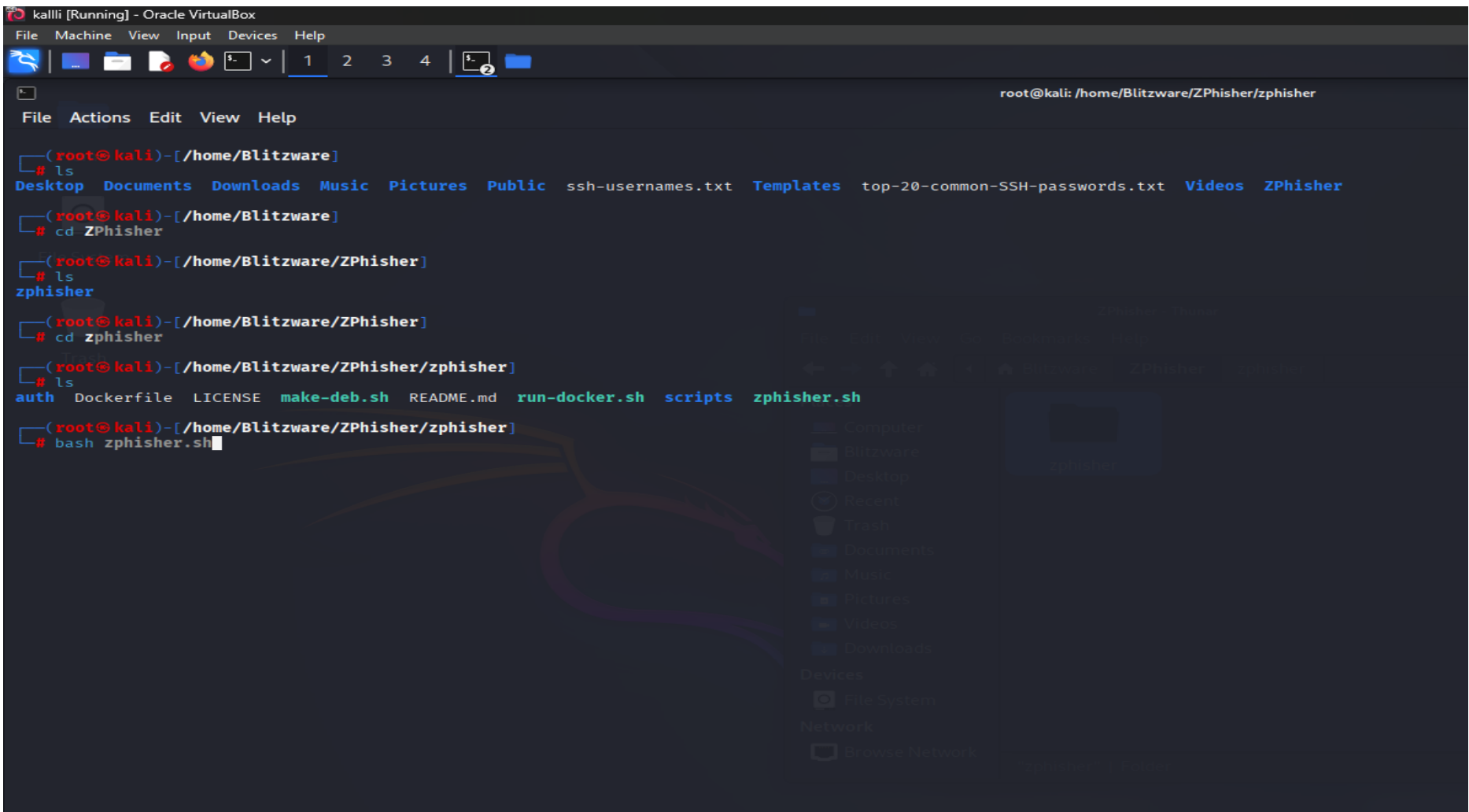
Component	Description
Host Machine	Kali Linux (running in VirtualBox)
Network Mode	Bridge Adapter (for proper tunnel access)
Phishing Tool	Zphisher (a social engineering toolkit)
Targeted Services	LinkedIn, Facebook
Tunnelling Services	Cloudflare (auto-generated by Zphisher)
Note	No real victim was involved. This was strictly for ethical and educational purposes.

Execution Steps

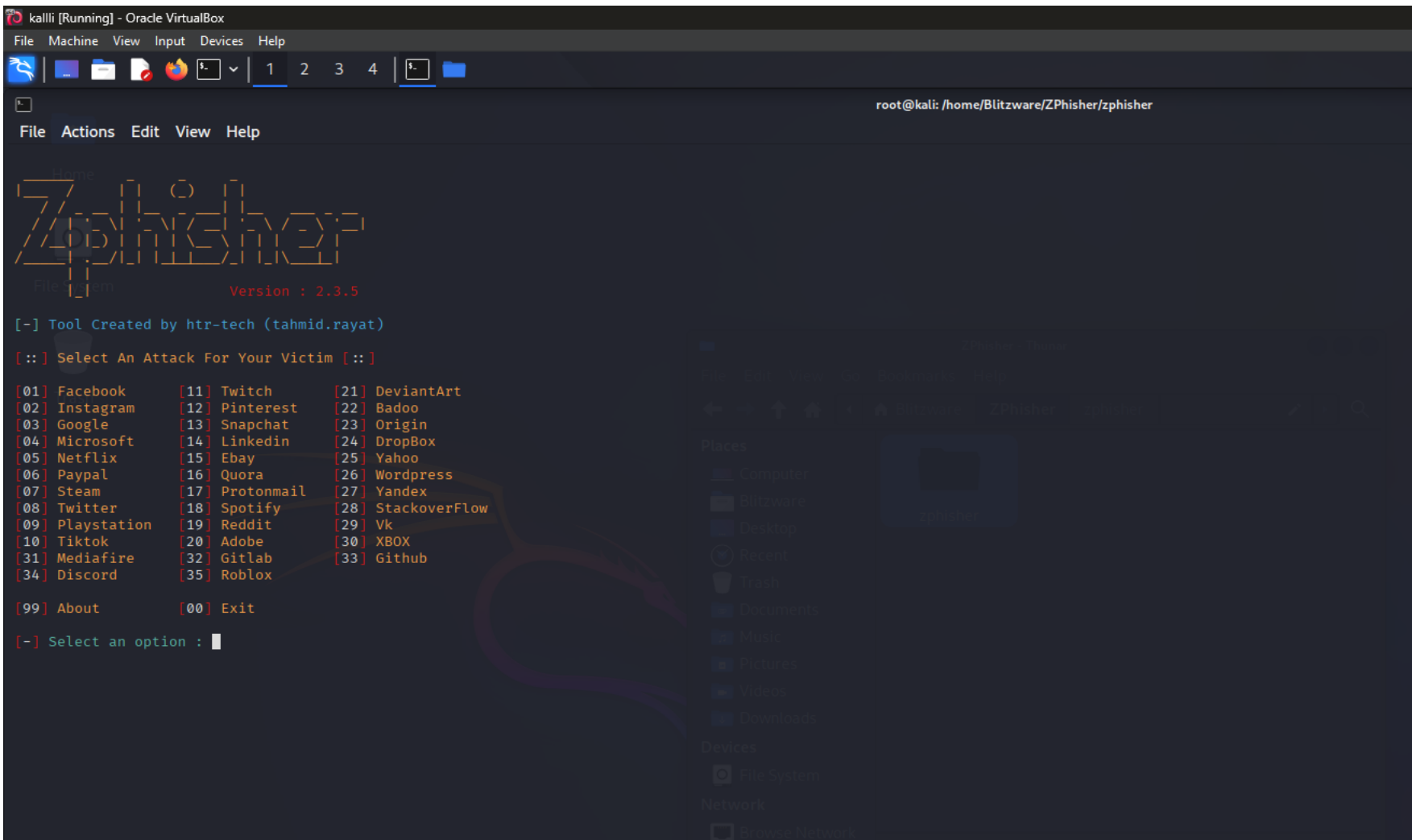
- Kali Linux was launched, and its version was verified for compatibility.



- A dedicated directory was created: /Zphisher.
- Zphisher was cloned and configured from its GitHub repository: <https://github.com/htr-tech/zphisher>
- The tool was executed via terminal using: bash zphisher.sh



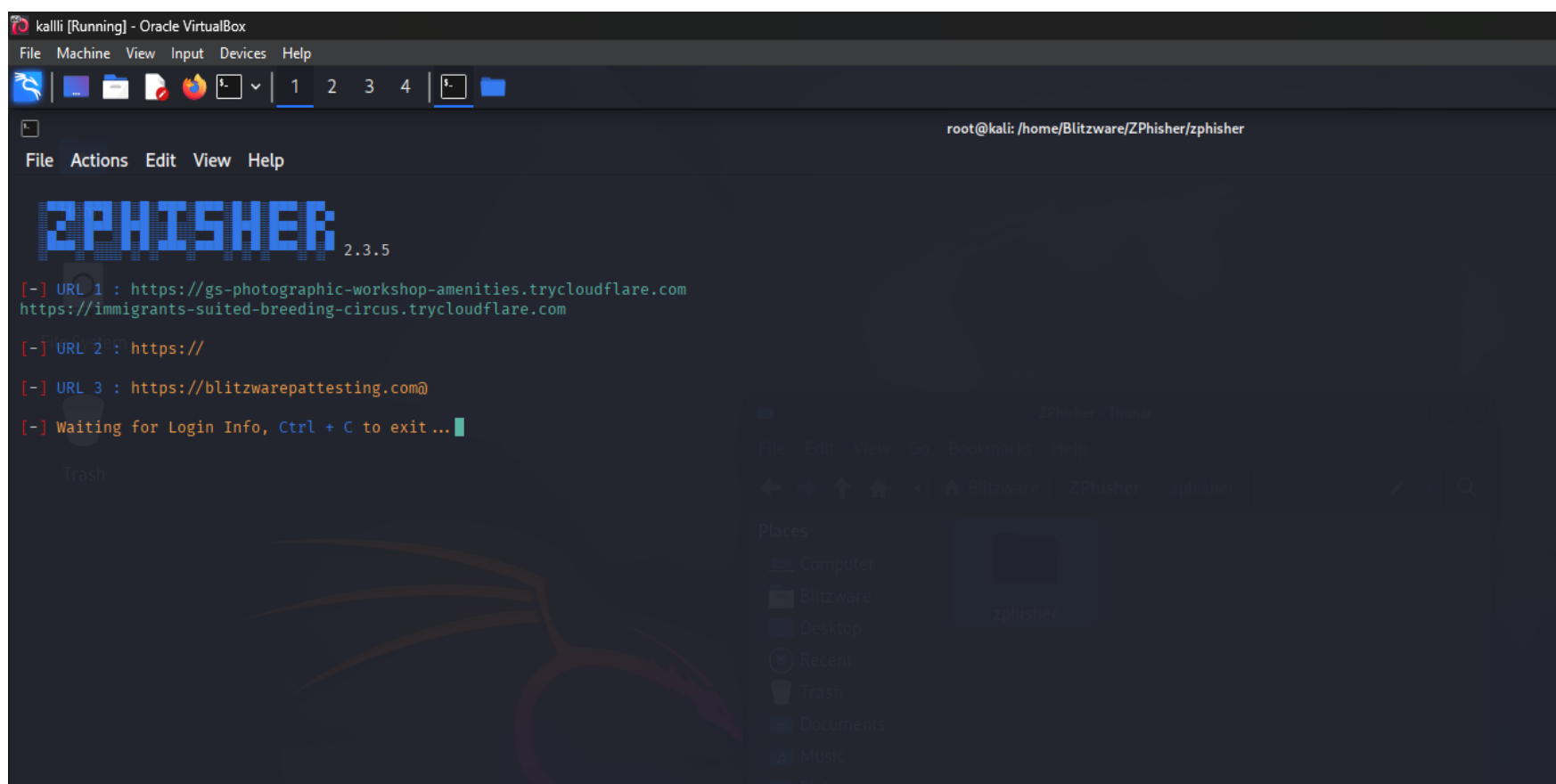
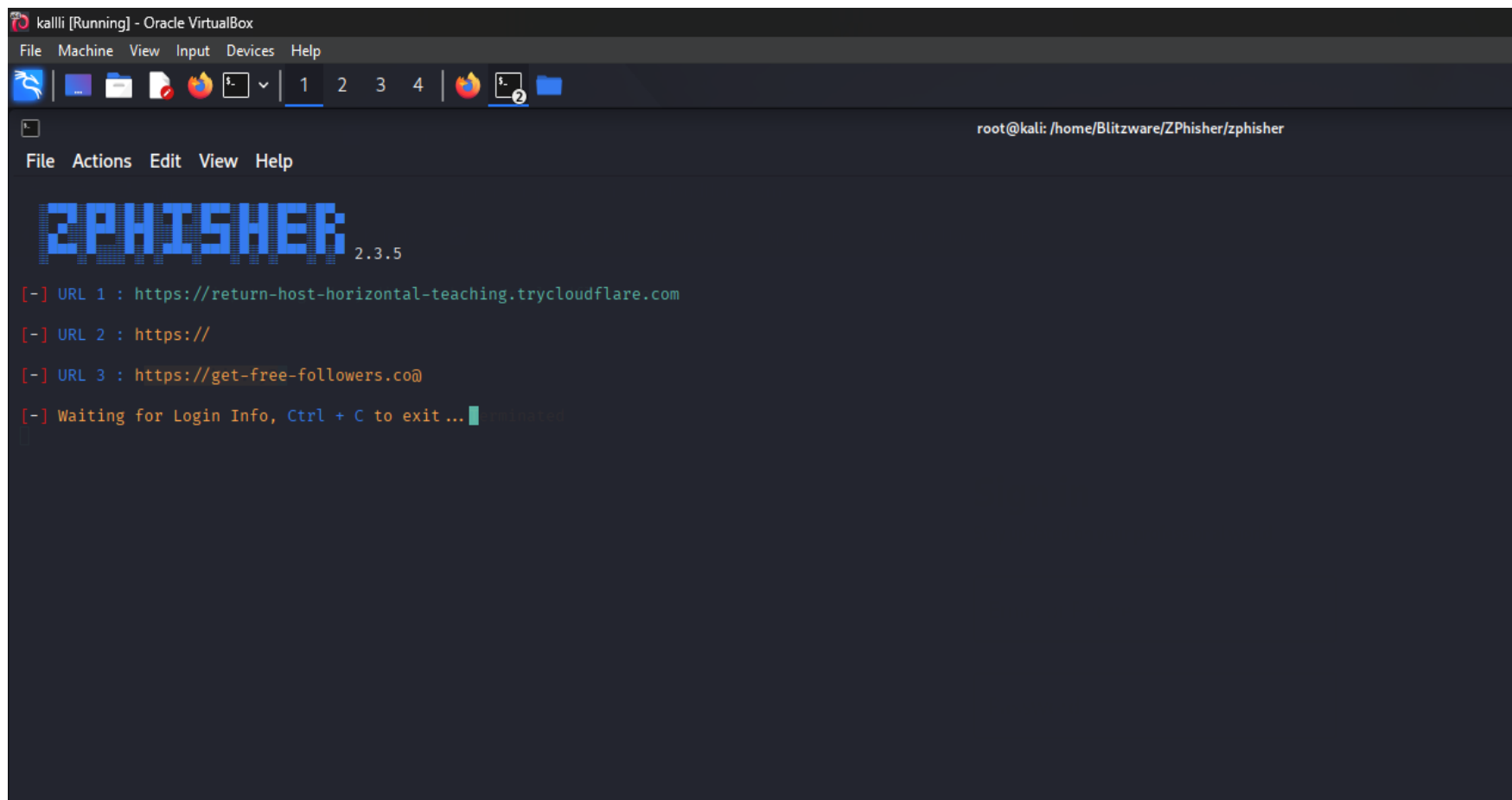
- The tool presented multiple platforms for phishing simulation. LinkedIn was selected first, followed by Facebook.



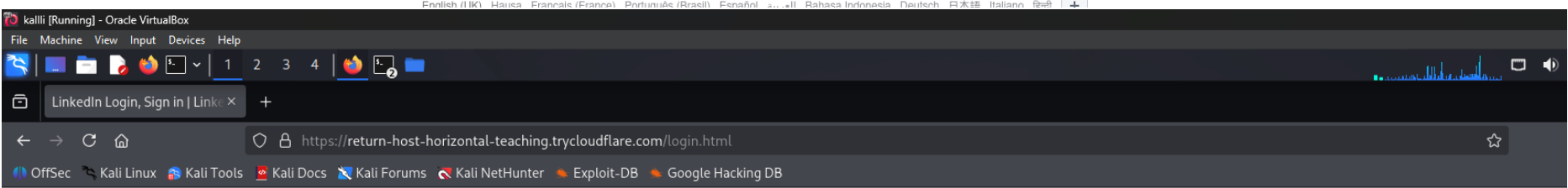
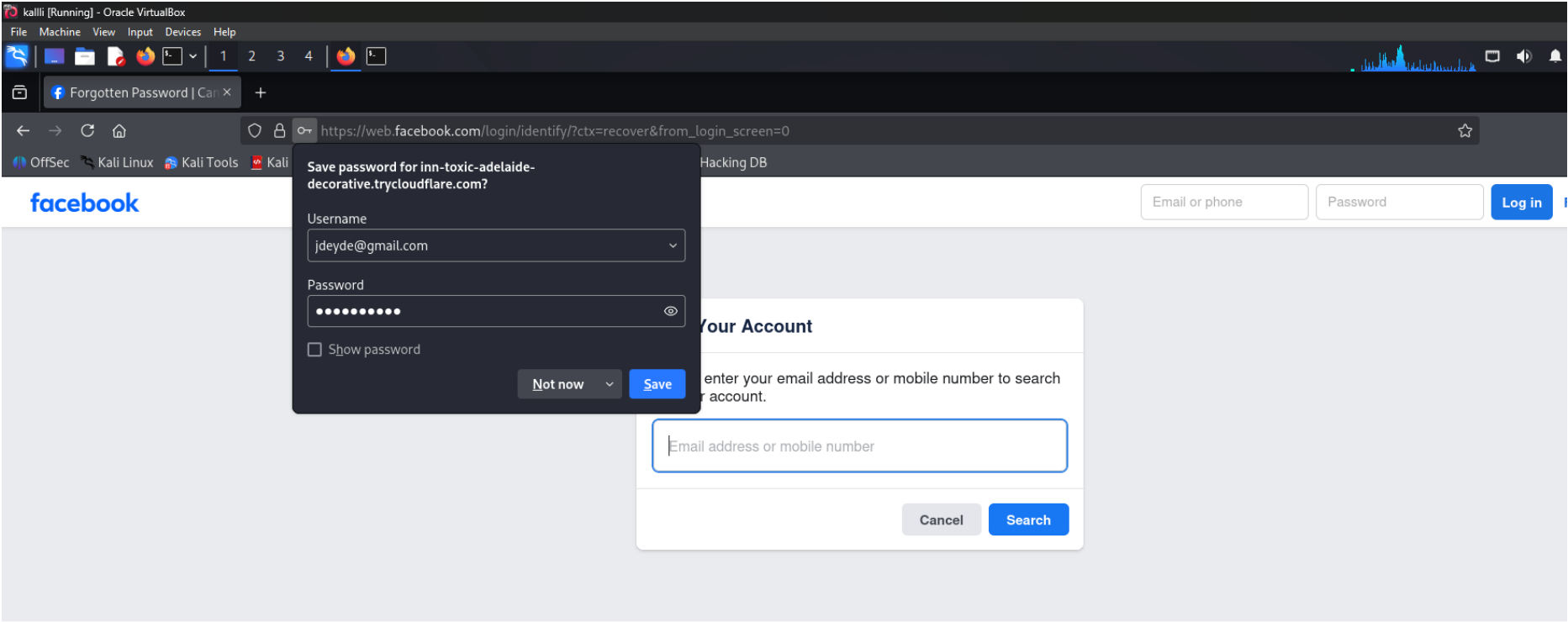
- Upon selecting a target, Zphisher generated multiple phishing URLs using tunneling options:
 - Localhost

➤ Cloudflare

- URLs were generated that could be used to access both the masked page to carry out the phishing.



- The Cloudflare URL was successful it hosted a fake login page of both LinkedIn and Facebook.



Sign in

Stay updated on your professional world

Email or Phone

Password [show](#)

[Forgot password?](#)

Sign in

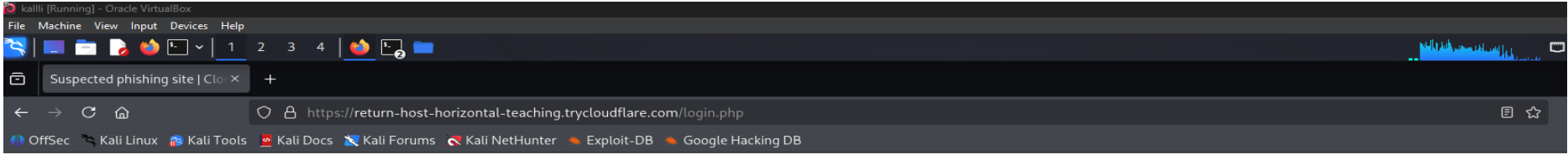
or

Sign in with Google

Sign in with Apple

New to LinkedIn? [Join now](#)

- When the LinkedIn phishing page was accessed, the browser flagged it as a suspected phishing site and blocked access.



!Suspected Phishing Site!

This link has been flagged as phishing. We have blocked it for your safety.

What is phishing?

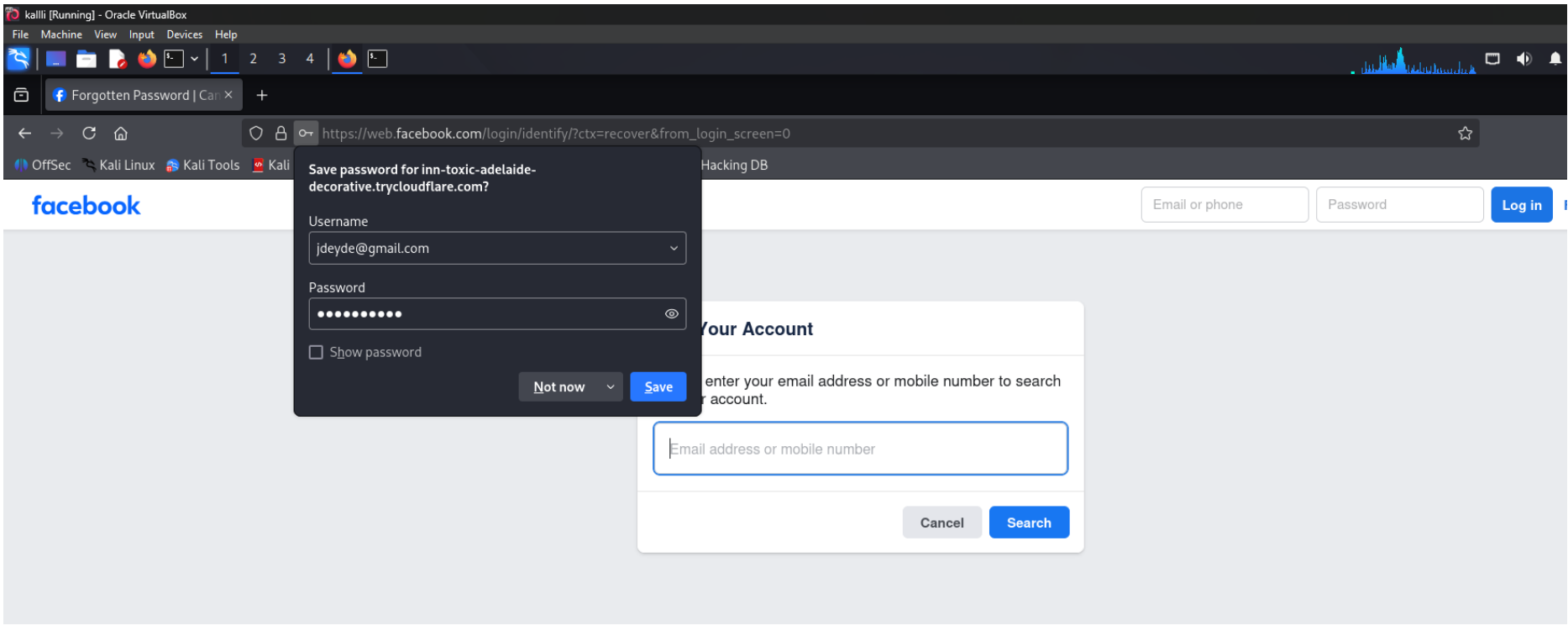
This link has been flagged as phishing. Phishing is an attempt to acquire personal information such as passwords and credit card details by pretending to be a trustworthy source.

What can I do?

If you're a visitor of this website
For now this site has been blocked. If you believe this is an error you can try again later.

If you're the owner of this website
If this is your quick tunnel and you want to dispute this block, contact qtabuse@cloudflare.com with the URL and a detailed explanation of its intended use.

- The Facebook phishing page was able to bypass the warning, load successfully, and capture data.



- Upon submission of dummy login credentials, the entered username was successfully captured and stored inside the auth folder on the attacking machine.

```
kalili [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@kali: /home/Blitzware/ZPhisher/zphisher/auth
File Actions Edit View Help
Desktop Documents Downloads Music ngrok-stable-linux-amd64.zip Pictures Public ssh-usernames.txt Templates top-20-common-SSH-passwords.txt
(root@kali)-[/home/Blitzware]
# cd ZPhisher
(root@kali)-[/home/Blitzware/ZPhisher]
# ls
zphisher
(root@kali)-[/home/Blitzware/ZPhisher]
# cd zphisher
(root@kali)-[/home/Blitzware/ZPhisher/zphisher]
# ls
auth Dockerfile LICENSE make-deb.sh README.md run-docker.sh scripts zphisher.sh
(root@kali)-[/home/Blitzware/ZPhisher/zphisher]
# cd auth
(root@kali)-[/home/Blitzware/ZPhisher/zphisher/auth]
# ls
ip.txt usernames.dat
(root@kali)-[/home/Blitzware/ZPhisher/zphisher/auth]
# cat ip.txt
IP:
Use /5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
IP:
Use /5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
IP:
Use /5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
IP:
Use /5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
IP:
Use /5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
IP:
Use /5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
IP:
Use /5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
IP:
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
(root@kali)-[/home/Blitzware/ZPhisher/zphisher/auth]
# cat usernames.dat
Facebook Username: jdeyde@gmail.com Pass: ripper2025
(root@kali)-[/home/Blitzware/ZPhisher/zphisher/auth]
#
```

Issues Encountered

- Not all the generated phishing links were functional. Only the Cloudflare-based tunnel link successfully hosted the phishing page.
- The browser's security system detected and blocked the LinkedIn phishing page, showcasing real-world browser defence mechanisms.

Ethical Consideration

This phishing simulation was conducted solely for educational and ethical learning purposes. No real users were targeted, and all tests were done within a closed lab environment to practice and understand adversarial techniques in a safe and responsible manner.

Next Steps & Recommendations

- Explore defensive countermeasures, such as:
- Browser hardening
 - Deploying Intrusion Detection Systems (IDS/IPS)
 - Conducting phishing awareness training simulations

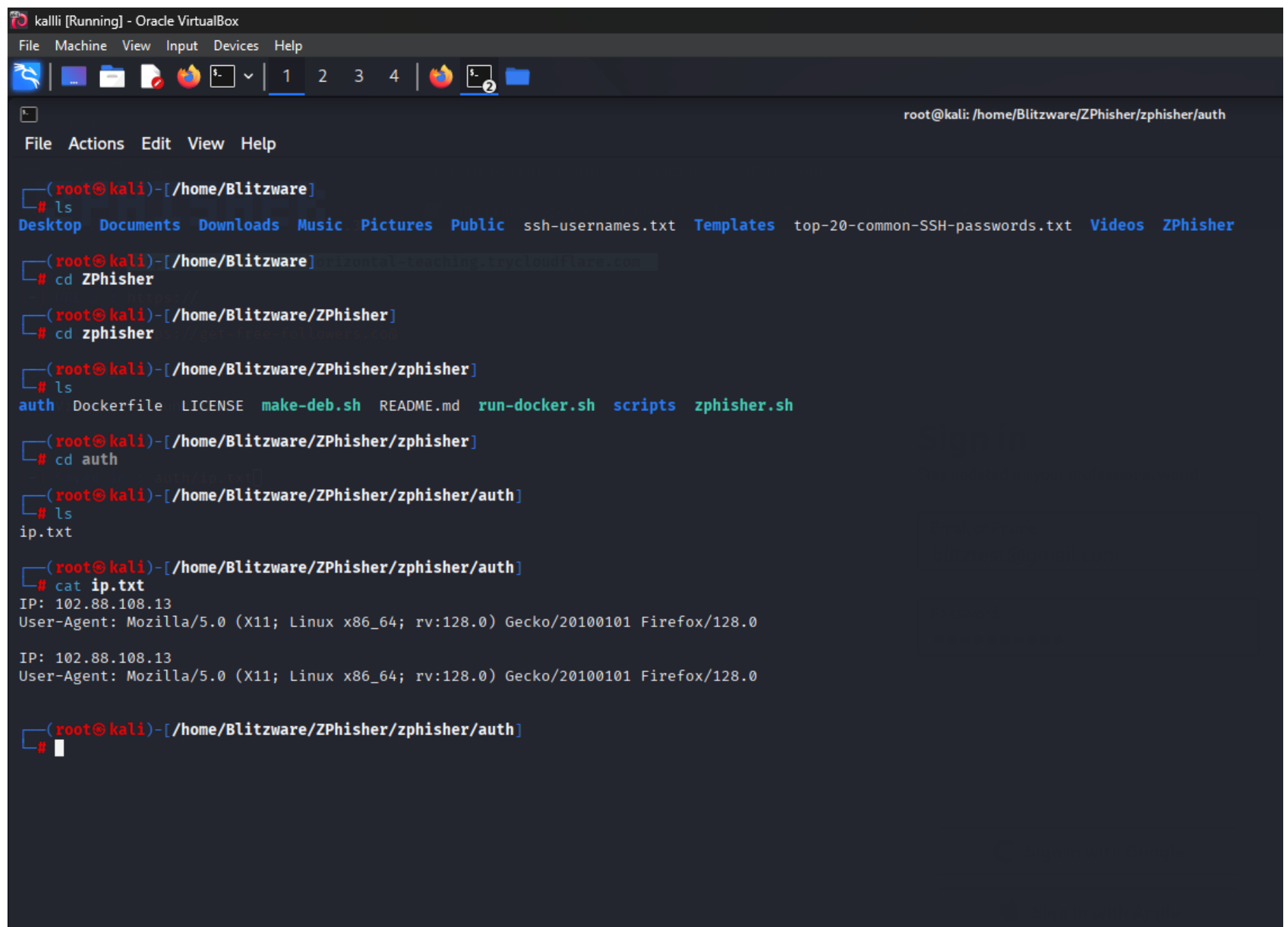
- Extend the lab to include email phishing simulations and payload delivery testing in a sandbox environment.

Conclusion

This simulation demonstrated how attackers can use open-source phishing kits like Zphisher to exploit user trust by mimicking familiar login pages. It also highlighted the importance of:

- Browser based phishing detection systems
- Network security awareness
- The role of tunnelling in bypassing local restrictions

Further exercises can involve defensive testing, such as setting up IDS/IPS, browser security hardening, or simulating phishing awareness responses.



```
kallli [Running] - Oracle VirtualBox
File Machine View Input Devices Help

root@kali: /home/Blitzware/ZPhisher/zphisher/auth

File Actions Edit View Help

(root@kali)-[/home/Blitzware]
# ls
Desktop Documents Downloads Music Pictures Public ssh-usernames.txt Templates top-20-common-SSH-passwords.txt Videos ZPhisher

(root@kali)-[/home/Blitzware]
# cd ZPhisher

(root@kali)-[/home/Blitzware/ZPhisher]
# cd zphisher

(root@kali)-[/home/Blitzware/ZPhisher/zphisher]
# ls
auth Dockerfile LICENSE make-deb.sh README.md run-docker.sh scripts zphisher.sh

(root@kali)-[/home/Blitzware/ZPhisher/zphisher]
# cd auth

(root@kali)-[/home/Blitzware/ZPhisher/zphisher/auth]
# ls
ip.txt

(root@kali)-[/home/Blitzware/ZPhisher/zphisher/auth]
# cat ip.txt
IP: 102.88.108.13
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0

IP: 102.88.108.13
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0

(root@kali)-[/home/Blitzware/ZPhisher/zphisher/auth]
#
```